International Journal of Research and Review
Vol. 9; Issue: 11; November 2022
Website: www.ijrrjournal.com
Review Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Data Security in Cloud Computing: A Research Perspective

Rachana CR

Associate Professor & Head, Department of Studies in Computer Science, First Grade College (Autonomous), PG Wing, Memorial Mahajana Education Centre, KRS Road, Metagalli, Mysuru-570016

DOI: https://doi.org/10.52403/ijrr.20221144

ABSTRACT

Security plays a very important role in the life of every living being. Today, in the 'Technology' engulfed businesses, data security is crucial for users and vendors alike. Cloud computing as a technology is the driving force behind all the financial transactions being completed every second across the globe. In the current context, Cloud data security is crucial and is of utmost importance. Data Security in the cloud refers to the technologies, policies, services, security controls that protect data in the cloud from loss, leakage or misuse through security breaches and unauthorized access. Securing data in the cloud is essential in e-commerce because attacks on the data can result in loss of revenue for businesses. Cyber criminals use advanced tools and techniques to steal information from the cloud servers for financial gain and other unscrupulous benefits. Securing data while it is at rest or in transit is most important for businesses. Efficient Data security tools and techniques must be applied to protect the data resident in the cloud. This paper closely examines the Issues and challenges of Data Security in Cloud Computing with reference to e-commerce.

Keywords: Challenges, Cloud Computing, Data Security, E-Commerce, Public Cloud.

INTRODUCTION

The 'Cloud' is used to describe servers with its associated services, software applications, databases, containers and workloads. They are accessed remotely through the internet. Cloud resources, such as databases, are flexible, in the sense that they can be quickly spun up or down based on the variable needs of the business. This feature of cloud allows the organization to manage surges in demand or seasonal spikes in a more timely and cost-effective way [1]. The Virtual Machines on the public cloud are sharing infrastructure, hardware and software with other cloud tenants. Cloud environments are divided into three categories. One is the private cloud, the Private cloud and the hybrid cloud. Private cloud environment is used exclusively by one customer and a public cloud is shared by more than one user. Hybrid cloud combines one or more public cloud and private cloud environments. Hybrid cloud gives the user the benefits of both private and public clouds [2]. It provides high scalability, virtually unlimited storage space, and flexible payment models. Just like public clouds, hybrid cloud environments are cost effective. Hybrid cloud is also highly secure; provides more flexibility and control over cloud resources just like in private cloud environments [4].

Two major trends have revolutionized the e-commerce industry [7]. They are: the mass use of mobile devices, and the rapid migration of data to the cloud. The cloud allows users to access the same files and applications from any device, from anywhere. The computing and storage of data takes place on the servers in the data centre, instead of locally on the user device. This also gives out an illusion of infinite resources to the users. Today, most of the e-Commerce sites have moved their business to cloud computing platforms and are operating through the cloud servers.

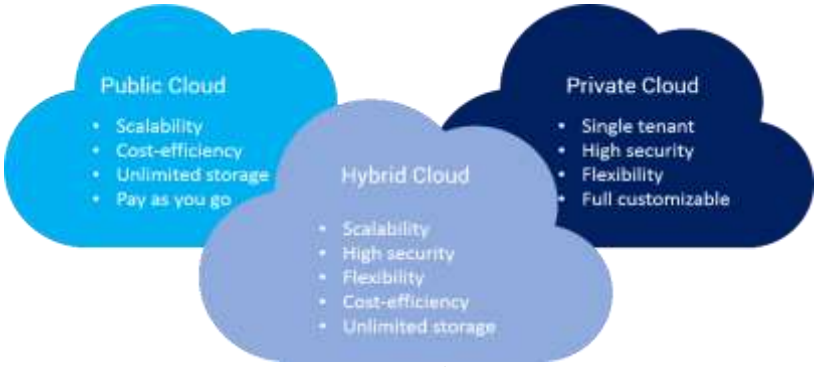

Fig 1: Types of Cloud

The feature of virtualization is one of the most important characteristics of cloud computing. To remain competitive in this evolving digital world, organizations must make strategic decisions with respect to cloud migration, cloud architecture, usage of public clouds, and cost management. So, we can see that the Businesses are increasingly turning to the cloud for their data storage and processing needs, and the trend is not going down soon. With the advent of new technologies more businesses will migrate to cloud to serve the best to its customers.

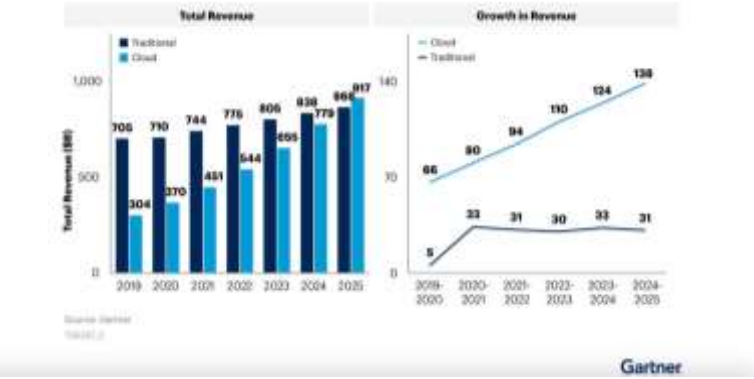

Fig 2: Sizing Cloud Shift worldwide, 2019-2025, Image: Gartner.

The scale of cloud spending continues to rise [17]. For the full year 2021, tech analyst IDC expects cloud infrastructure spending to have grown 8.3% compared to 2020 to $71.8 billion, while non-cloud infrastructure is expected to grow just 1.9% to $58.4 billion. Long term, the analyst expects spending on compute and storage cloud infrastructure to see a compound annual growth rate of 12.4% over the 2020-2025 period, reaching $118.8 billion in 2025, and it will account for 67.0% of total compute and storage infrastructure spend. Spending on non-cloud infrastructure will be relatively flat in comparison and reach $58.6 billion in 2025, Steve Ranger[17].

As per the Flexera 2022 State of the Cloud Report [8], Cloud costs continue to grow. The optimized use of existing cloud is the top initiative.

Fig 3: Flexera 2022 state of the cloud report.

A recent industry report states that the e-commerce will account for 20.4% of global retail sales by the end of 2022, up from only 10% five years ago. This means that the e-commerce space is going to get even more crowded.

One of the reasons for ecommerce businesses gaining up sales was Covid 19 [15] which exposed many shoppers to explore the benefits and ease of online shopping. A key factor in driving sales for online fashion and apparel stores is Influencer marketing. Influencer marketing is all about a brand collaborating with an online influencer to market one of its products or services [21]. Ecommerce businesses understood that collaboration with influencers can help them double their sales [16].

It is interesting to note that, 41% of digital shoppers have stated that they are very likely or extremely likely to drop a brand if the trust of that brand is deemed damaged. 59% of digital shoppers would lose trust in a business after having an unsatisfactory experience. $4.4 trillion the amount that is set to be spent on digital transformation among businesses, spurred on by monumental changes in buying behaviour and supply chain disruption brought by the pandemic. 12% drop in worldwide artificial intelligence (AI) funding during the first quarter of 2022, representing $15.1 billion, which has helped to transform multiple industries from commerce and healthcare to logistics [18].

E-commerce Data Security Issues and Challenges

Ecommerce sites will always be the most targeted place of cybercriminals. It is a treasure house of personal and financial data. Any compromise in the data will result in great financial losses to the businesses.

The most important risks of Data breach which concerns e-commerce companies are many.

Fig 4: Major Security challenges businesses faced in 2021, Source: Webscale

About 32.4% of all attacks is experienced by e-commerce sites. 50% of small e-Commerce store owners are of the opinion that the attacks are becoming severe. Reports [20] demonstrate that 29% of traffic accessing a website consists of malicious requests. Such serious types of attacks have contributed to significant losses in financials, market shares, and reputation of the businesses. Almost 60% of small e-Commerce stores that experience cybercrimes don't survive more than six months [19].

Distributed denial of service (DDoS) attacks continued to be seen as a critical issue as well - even after the substantial increase in DDoS defence investments following the emergence of the Mirai botnet back in 2016 [3]. A distributed denial-of-service (DDoS) attack occurs when multiple systems are operating together to attack the e-commerce site and server. The e-commerce site is flooded with malicious queries that stop the site from working properly making it inoperable. These attacks are disruptive, costly and affect overall sales [5].

The common Cloud-based attacks that can affect businesses include [9]:

1. Crypto jacking. Malware is injected into the e-Commerce website's pages. The attacker will find a weakness in the site's security and exploit it to gain access to parts of the site that is secure.

2. E-skimming [13]. This attack involves the introduction of code onto a web page for the purpose of intercepting sensitive user information as the user of the web page is entering the data into the website form. The type of information stolen by the attacker includes Credit Card Data, Social Security Numbers, Bank Account Details, And Other Personally Identifiable Information (PII).
3. Unauthorized access. This leads to modification of data by unauthorized users, data breach, data loss, stealing trade secrets of businesses.
4. Transaction Fraud [12]. Number of transactions happen in a second on e-commerce websites. Customers trust the transaction process hence, prefer online payments. But a transaction fraud can happen in two ways. In the First type, the Credit card fraud happens when the attacker makes an unauthorized purchase with credit card information that is stolen from the authorized user. Stolen credit card numbers are often obtained through phishing attacks. The cyber attackers contact the users/consumers by phone or email and attempt to convince them to get the credit card information.
   In the second type, transactions are carried out using insecure systems that get redirected or interrupted. Users must be more alert and they must be educated about the various steps to follow while completing an online transaction securely. There are many advertisements by the government now a day which are alerting consumers regarding the safe ways to buy goods and services online.
5. Brute Force Attack [11]. This is the simplest method to gain access to a server or website. The attack involves attempting several usernames and passwords combinations repeatedly until it gains access into the account. Brute force attacks usually target the administrator's panel of an online store.
6. SQL injection. If the ecommerce website insecurely stores data in the SQL database and if it is not properly validated, a malicious query can be injected into a packaged payload can give the attacker access to view and manipulate any information in the database [6].
7. Cross-Site Scripting (XSS) [13]. Attackers make use of the loopholes and gaps within an application to insert malicious codes/scripts which get activated when the users load the website. Typically, malicious JavaScript codes are injected into the website. While these codes will not affect the website itself, the end-users will get exposed to phishing scams, malware once they visit and load the compromised website.

Further the most usual types of cloud misconfigurations which lead to risks include [10]:

1. Muddled Data Access. This happens when confidential data is excluded in the open and requires no authorization.
2. Common Cloud Security Settings of the server with standard access management and availability of data.
3. Mismatched Access Management. This is when a person who is not authorized, accidentally gains access to essential data.

Ecommerce Security:

The 6 pillars which influence the overall ecommerce business cybersecurity include:

1. Authentication ensures that the vendors and customers prove their identity for a transaction to occur safely.
2. Integrity maintains the information's consistency and accuracy, and assures that the data has not been modified without authorization.
3. Privacy refers to protecting consumers' data from unauthorized access.
4. Non-repudiation confirms that both vendors and customers have received the information exchanged with each other. Neither can deny the recorded transactions.

5. Availability of the e-Commerce websites increases online visibility, search engine rankings, and site traffic.
6. Compliance refers to the industry regulations and standards that e-Commerce businesses should stick to, in order to minimize risks related to data breach security and avoid penalties for non-compliance.

There are few good ways to make sure the data on the cloud is safe.

1. Educate the users, employees about phishing attacks. It is effortless to access the data on the cloud if the username and password is obtained by tricking the user or the employee of the organization. It must be made sure that all the employees know that they should not click on links in email unless they are sure of the authenticity of the sender. Few phishing emails look very authentic.
2. two-factor authentication [14]. This process might be time-consuming for the authentic users to verify every time they login from a new device. But, it is definitely worth it. Two factor authentication is as simple as asking security questions or it could be requiring to submit the verification code sent to their phone. Generally, Device-based authentication is most secure.
3. Set right access controls. If an employee in the organization is terminated, his/her access to the files must be immediately controlled. This should happen before any harm can be done to the organization data. Access to data must be granted to the people who are authenticated users of that data.
4. Maintain backups. It is worth keeping extra backup outside the normal cloud provider, especially for crucial/sensitive data. Some data must be stored on a physical drive that is protected by the site security. A Good backup policy protects the data from ransom ware and similar attacks. It also protects from data destruction.
5. Employ the right cloud provider. It is important to know from the cloud provider about the security features and how they serve to backup data stored in the cloud.

CONCLUSION

Electronic commerce is growing rapidly and penetrating as a technological revolution very robustly in the lives of people in remote areas as well. A number of technologies and the internet have converged to facilitate the rapid growth of e-commerce. The rapid advances in technology along with the rapid acceleration in networking and the continuous development of sophisticated software have revolutionized the way business is done. Cloud Computing has become one of the essential platforms which are providing support for small and large businesses. Likewise, e-commerce companies have experienced the potential of the cloud in providing safe and comfortable user experience.

As cloud use can be ideal for any e-Commerce business, one obstacle that the businesses are facing is the variety of security risks. These risks can cause severe negative impacts that can severely damage the reputation and financial positions of businesses. Some of the cloud security risks that e-Commerce companies are encountering when using cloud computing are unsecured APIs, data loss, malware attacks, and misconfigured services. To keep security threats at bay, businesses should adopt several e-Commerce security measures and protocols. With an SSL certificate for a website, the e-commerce site can move from HTTP to HTTPS for security benefits. Multi-factor authentication (MFA) feature implementation by the retailers will ensure consumer authentication.

Conflict of Interest: None

REFERENCES

1. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-data-security/

2. Mike Tierney, Data Security in Cloud Computing: Key Components, Published: July 2, 2020, Updated: January 13, 2022.
3. Paul Nicholson, Cloud growth brings security concerns for e-commerce, https://www.securitymagazine.com/articles/97269-cloud-growth-brings-security-concerns-for-e-commerce, March 17, 2022.
4. Alibaba Clouder, Public Cloud vs Private Cloud vs Hybrid Cloud: What Is the Difference, https://www.alibabacloud.com/blog/public-cloud-vs-private-cloud-vs-hybrid-cloud-what-is-the-difference_597486, March 18, 2021.
5. Karl Wittig, E-commerce Security: 5 Ways to Enhance Data Protection During the Shopping Season, https://www.loginradius.com/blog/identity/ecommerce-security/
6. https://www.bigcommerce.com/articles/ecommmerce/ecommerce-website-security/
7. Aslam Hasan Khan, Future of E-Commerce: How Cloud Computing Will Affect It, https://yourstory.com/mystory/future-ecommerce-cloud-computing-affect/amp, April 12, 2022, Updated on:Apr 12, 2022, 12:38 PM GMT+5:30.
8. https://info.flexera.com/CM-REPORT-State-of-the-Cloud
9. https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions
10. https://ecommercefastlane.com/5-cloud-security-risks-for-ecommerce-companies/
11. https://star-knowledge.com/blog/ecommerce-security-threats-issues-solutions/
12. https://phoenixnap.com/blog/ecommerce-security-threats
13. Basics of eCommerce Security & Best Practices you should Follow (webscoot.io)
14. 7 Ways to Prevent Data Leaks in the Cloud - OTAVA
15. Percy Hung, Forbes Councils Member, E-Commerce Trends 2022: What The Future Holds (forbes.com), Mar 14, 2022,10:15am EDT.
16. Effective Growth Hacks For Online ECommerce Stores In 2022 (the-next-tech.com)
17. What is cloud computing? Everything you need to know about the cloud explained | ZDNET
18. Argano UV, This Week in eCommerce Data: May 27th, 2022, https://weareuv.com/this-week-in-ecommerce-data-may-27th-2022/
19. Jinson Varghese, Ecommerce Security: Importance, Issues & Protection Measures, Updated on: July 3, 2022, https://www.getastra.com/blog/knowledge-base/ecommerce-security/
20. https://www.getastra.com/blog/cms/hacking-statistics/
21. Werner Geyser, What is Influencer Marketing? – The Ultimate Guide for 2022, Last Updated: August 16th, 2022, https://influencermarketinghub.com/influencer-marketing/.

How to cite this article: Rachana CR. Data security in cloud computing: a research perspective. *International Journal of Research and Review*. 2022; 9(11): 325-330.
DOI: *https://doi.org/10.52403/ijrr.20221144*

******